SZR: Häufig gestellte Fragen zur Absenderreife

Inhalt

Einführung

Cisco Talos Sender Domain Reputation (SDR) ist ein Cloud-Service, der ein Reputationsprotokoll für E-Mail-Nachrichten auf Basis der Domäne eines Absenders und anderer Attribute bereitstellt. Diese domänenbasierte Reputationsanalyse ermöglicht eine höhere Spam-Abfangrate, indem sie über die Reputation von gemeinsam genutzten IP-Adressen, Hosting- oder Infrastrukturanbietern hinausblickt und Verdicts basierend auf Funktionen ableitet, die mit vollqualifizierten Domänennamen (FQDNs) und anderen Absenderinformationen im Simple Mail Transfer Protocol (SMTP)-Gespräch und E-Mail-Headern verknüpft sind.

F. Was bedeutet "Absenderreife"?

Antwort: Domain Age ist ein irreführender Begriff und wurde kürzlich in Sender Maturity (siehe aktuelles SDR Whitepaper) geändert. Wir sagen, dass es irreführend ist, weil es nicht in der Tat dem Alter einer Domain entspricht, wie es durch das Registrierungsdatum der Domain reflektiert wird. Die Absenderreife wird im ESA-Verfolgungsprotokoll vorerst weiterhin als Domain Age (Domänenzeitalter) bezeichnet. Dies kann sich jedoch in einer zukünftigen Version ändern. Talos verwendet mehrere interne Datenquellen, um die Absenderreife abzuleiten.

> **Hinweis**:Talos kann keine Details über die Quellen preisgeben, die zum Ableiten der Domain-Reife verwendet werden, außer den Informationen, die bereits im neuesten SDR-Whitepaper veröffentlicht wurden, da es sich hierbei um proprietäre Informationen von Cisco Talos handelt.

F. Kann Talos die Absenderreife manuell ändern?

Antwort: Nein, Talos ändert die Absenderreife einer Domäne nicht manuell. Die Absenderreife ändert sich automatisch, basierend auf Änderungen im internen Datenkontext, der zu einem bestimmten Zeitpunkt für die Domäne verfügbar ist.

F. Warum hat eine Domäne nach kurzer Zeit eine andere Senderreife?

In der ersten Nachricht wird eine Absenderlaufzeit von 10 Monaten angezeigt:

```
02 Apr 2020 09:40:38 (GMT +02:00)
Message 82366447 Domains for which SDR is requested: reverse DNS host: xxxxxxx.com, helo:
xxxxxxx.com, env-from: xxxxxxx.net, header_from: xxxxxxx.net, reply_to: Not Present
```

02 Apr 2020 09:40:38 (GMT +02:00)
Message 82366447 Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest **Domain Age: 10 months 15 days** for domain: xxxxxxx.net

In der zweiten Nachricht wird eine Absenderlaufzeit von 13 Tagen angezeigt, **obwohl es sich um dieselbe Domäne handelt**:

12 May 2020 09:54:12 (GMT +02:00)
Message 86558836 Domains for which SDR is requested: reverse DNS host: xxxxxxx.com, helo: xxxxxxx.com, env-from: xxxxxxx.net, header_from: xxxxxxx.net, reply_to: Not Present

12 May 2020 09:54:12 (GMT +02:00)
Message 86558836 Consolidated Sender Reputation: Weak, Threat Category: N/A. Youngest **Domain Age: 13 days** for domain: xxxxxxx.net

Antwort: Die Quellen, die Talos zum Ableiten der Senderreife verwendet, können sich je nach Änderungen im internen Datenkontext einer Domäne ändern. Dies kann dazu führen, dass verschiedene Domain Age-Labels für eine bestimmte Domäne im ESA-Nachrichtenüberwachungsprotokoll angezeigt werden, wie im obigen Beispiel gezeigt. Obwohl diese Änderungen selten sind, sind sie zu erwarten und erfordern kein Eingreifen.